UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/758,024	01/16/2004	Pascal Viger	01807.002565	6231

5514 7590 06/29/2007

FITZPATRICK CELLA HARPER & SCINTO
30 ROCKEFELLER PLAZA
NEW YORK, NY 10112

EXAMINER	
SCHMIDT, KARI L	

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
06/29/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/758,024	VIGER ET AL.	
	Examiner	Art Unit	
	Kari L. Schmidt	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 January 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-60* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-60* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 January 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *4/12/2004, 6/8/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Specification

Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

Claim Objections

Claims 52-59 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. Claims 52, 54, 56, and 58 are referring to an information carrier, which doesn't further limit Claims 1, 8, 12, and 20. Claims 53, 55, 57, and 59 are referring to a computer product program stored on an information carrier, which doesn't further limit Claims 1, 8, 12, and 20.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

Claims 8- 9 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 8 claims "a device manufacturing apparatus" and Claim 9 claims "an exposure apparatus for exposing a substrate to a pattern" both claims don't particularly point out and distinctly claim the subject matter. Also, not sure what it means/not clear when Claim 9 uses the terms "exposure" and "pattern".

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 52-59 are rejected under 35 U.S.C. 101 because claims 52-59 are directed to "computer program products" stored in a "information carrier". Generally, functional descriptive material, such as a computer program, is statutory when it is stored on a tangible computer readable medium. See MPEP § 2106 IV.B.I (a). A computer program listing on a sheet of paper is not considered to provide functionality, and is therefore considered to be merely a computer program per se, which is non-statutory subject matter. Further, "transmission media" such as "communications links"

as broadly defined may include non-tangible media such as signals, which are also considered non-statutory. When a claim encompasses both statutory and non-statutory subject matter, the claim as a whole is directed to non-statutory subject matter.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Claims 1-60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ross Jr. (US 5, 812, 671) in view of Herpel et al. (EP 1 045 386 A1).

Regarding Claim 1, Ross teaches a method of transferring at least one digital signal representing media content data in a communication network, the network comprising a client server device connected to at least one client station, at least one destination server device connected to at least one destination station wherein, when the client station receives a request to transfer a digital signal intended for at least one destination station, the client server device: obtains a first encryption key further to the transfer request; obtains the digital signal; encodes said digital signal with the first encryption key obtained; encodes the first encryption key with a second encryption key associated with the destination server device connected to the corresponding destination station; transfers the encoded digital signal to said destination server device; transfers the encoded first encryption key to said destination server device (Figure 2: column 3, lines 35-53: "node A is the client and node B is the destination.. file is transferred to A's network server interface, where a decision can be executed to send the file encrypted..").

Regarding Claim 2, Ross teaches a method according to Claim 1, wherein the client server device also determines, from the transfer request, whether information representing at least one restriction on use by a destination station exists and, if so, encodes the information representing at least one restriction with the second key associated with the destination server device of the corresponding destination station and transfers the encoded information to the destination server device (Figure 2: column 3, lines 54-column 4, line 3: "if B is a client, B's algorithm and key are loaded

into the encryption server and encrypted file... at node B the encrypted file is identified as a file having been sent from the encryption gateway, appropriate decryption algorithm and key are used to decrypt the file..." and Abstract: "node A encrypted the message using party A's secret key and encryption algorithm, copies of which are stored at the network gateway... Party A sends the encrypted message, addressed to party B, initially to the gateway. The gateway decrypts the message, using party A's secret key and algorithm and then encrypted the decrypted message using party's B secret key and algorithm.. message can be digital signal for media file").

Regarding Claim 3, Ross a method according to Claim 1, wherein the said digital signal is stored in advance on the client server (column 1, lines 60 – column 2, line 10: "party A encrypts the message using party A's secret key and encryption algorithm, copies of which are stored at the network gateway..").

Regarding Claim 4, Ross teaches a method according to Claim 1, wherein the transfer of the encoded signal to the said destination station is made by means of a centralized server device connected to the network (column 1, lines 14-20: "number of systems in use which encrypt and decrypt message transmitted over public network..." and Figure 1 and column 2, lines 30-65: "nodes A and B includes application programs for encryption/decryption and a suitable network interface program for coupling the node to a network... ").

Regarding Claim 5, Ross teaches a method according to Claim 1, wherein the first key is a secret key and the second key is a public key associated with the destination server device (column 1, lines 37-50 and column 2, lines 53-65: "public key, a receiving party (destination server device) can decipher a message without access to the sender's secret key (client)...").

Regarding Claim 6, Ross teaches a method according to Claim 5, wherein the public key is obtained by reading a storage means of the client server device or by generating a request on the communication network to the centralized server device or the destination server device (column 2, lines 53-65: "secure communications encryption gateway...").

Regarding Claim 8, Ross teaches a method of transferring at least one first digital signal representing media content data and which has been encoded using a first encryption key, in a communication network, the network comprising a client server device, and at least one destination server device connected to at least one destination station, wherein, when the client server device transfers the at least one digital signal encoded with the first encryption key to the at least one destination server device connected to the at least one destination terminal, the destination server device: stores the signal transmitted by the client server device; obtains the first encryption key by decoding, by means of a second key, a message received from the client server device,

decodes the stored digital signal by means of the first encryption key, and transfers at least one second decoded digital signal representing a sub-part of the first digital signal representing media content data to at least one destination station (column 1, lines 60-67: " stores the current encryption/decryption algorithms and keys for parties registered with the network secure communications gateway.." Figure 2: column 3, lines 35-53: "node A is the client and node B is the destination.. file is transferred to A's network server interface, where a decision can be executed to send the file encrypted.." and Figure 2: column 3, lines 54-column 4, line 3: "if B is a client, B's algorithm and key are loaded into the encryption server and encrypted file... at node B the encrypted file is identified as a file having been sent from the encryption gateway, appropriate decryption algorithm and key are used to decrypt the file..." and Abstract: "node A encrypted the message using party A's secret key and encryption algorithm, copies of which are stored at the network gateway... Party A sends the encrypted message, addressed to party B, initially to the gateway. The gateway decrypts the message, using party A's secret key and algorithm and then encrypted the decrypted message using party's B secret key and algorithm..").

Regarding Claim 11, Ross teaches a method according to Claim 8, wherein, on reception of a request to transfer the signal transmitted by the client server device to another destination station not associated with the destination server device, the destination server device obtains a third key associated with the destination server

device associated with the other destination station, encodes the first key with the third key and transfers the first digital signal encoded with the first key and the first key encoded with the third key (Abstract: "node A encrypted the message using party A's secret key and encryption algorithm, copies of which are stored at the network gateway... Party A sends the encrypted message, addressed to party B, initially to the gateway. The gateway decrypts the message, using party A's secret key and algorithm and then encrypted the decrypted message using party's B secret key and algorithm...").

Regarding Claim 12, Ross teaches a method for the transfer of at least one digital signal representing media content data in a communication network between a client module and at least one destination module, the modules being connected to the network, wherein it receives a request to transfer the digital signal to at least one destination module, the client module: - obtains the digital signal obtains a first encryption key; encodes the digital signal with the first encryption key; obtains information for the restriction on the use of the digital signal by the destination module, for which the digital signal is intended to be sent; encodes the first encryption key and the use restriction information with a second encryption key associated with destination module; transfers the encoded digital signal to the destination module; transfers the first encryption key and the use restriction information encoded with the second encryption key to the destination module (column 1, lines 60-67: " stores the current encryption/decryption algorithms and keys for parties registered with the network secure

communications gateway.." Figure 2: column 3, lines 35-53: "node A is the client and node B is the destination.. file is transferred to A's network server interface, where a decision can be executed to send the file encrypted.." and Figure 2: column 3, lines 54-column 4, line 3: "if B is a client, B's algorithm and key are loaded into the encryption server and encrypted file... at node B the encrypted file is identified as a file having been sent from the encryption gateway, appropriate decryption algorithm and key are used to decrypt the file..." and Abstract: "node A encrypted the message using party A's secret key and encryption algorithm, copies of which are stored at the network gateway... Party A sends the encrypted message, addressed to party B, initially to the gateway. The gateway decrypts the message, using party A's secret key and algorithm and then encrypted the decrypted message using party's B secret key and algorithm..").

Regarding Claim 13, Ross teaches a method for the transfer of at least one digital according to Claim 12, wherein the destination module comprises a destination server connected to the network and at least one destination client connected to the destination server (Figure 2: column 3, lines 35-53: "node A is the client and node B is the destination... file is transferred to A's network server interface, where a decision can be executed to send the file encrypted..").

Regarding Claim 14, Ross teaches a method for the transfer of at least one digital signal according to Claim 13, wherein the second encryption key is associated with the destination server (Abstract: "node A encrypted the message using party A's

secret key and encryption algorithm, copies of which are stored at the network gateway... Party A sends the encrypted message, addressed to party B, initially to the gateway. The gateway decrypts the message, using party A's secret key and algorithm and then encrypted the decrypted message using party's B secret key and algorithm...").

Regarding Claim 17, Ross teaches a method for the transfer of at least one digital signal according to Claim 12, wherein the first key is a secret key, and the second key is a public key associated with the destination module (Abstract: "node A encrypted the message using party A's secret key and encryption algorithm, copies of which are stored at the network gateway... Party A sends the encrypted message, addressed to party B, initially to the gateway. The gateway decrypts the message, using party A's secret key and algorithm and then encrypted the decrypted message using party's B secret key and algorithm..." and column 3, lines 35 – column 4, line 4).

Regarding Claim 18, Ross teaches a method for the transfer of at least one digital signal according to Claim 17, wherein the public key is obtained by reading by reading storage means of the client module or by generating a request on the communication network to a centralized server or to the destination module (Figure 1, column 2, lines 53-65: "secure communications encryption gateway..." and Figure 2: column 3, lines 35-53: "node A is the client and node B is the destination... file is

transferred to A's network server interface, where a decision can be executed to send the file encrypted.." and Figure 2: column 3, lines 54-column 4, line 3: "if B is a client, B's algorithm and key are loaded into the encryption server and encrypted file... at node B the encrypted file is identified as a file having been sent from the encryption gateway, appropriate decryption algorithm and key are used to decrypt the file...").

Regarding Claim 19, Ross teaches a method for the transfer of at least one digital signal according to Claim 12, wherein the use restriction information comprises a request for the destination module to transfer the digital signal encoded with the first key to at least a second destination module (Figure 1 and column 2, lines 30- column 3, line 23).

Regarding Claim 20, Ross teaches a method for the transfer of at least one first digital signal representing digital media content data and which has been encoded using a first encryption key, in a communication network between a client module and at least one destination module, the modules being connected to the network, wherein, when the client module transfers the encoded first digital signal to the destination module, the destination module: stores the first digital signal encoded with the first key; obtains the first key and information for the restriction on the use of the digital signal by the destination module, by decoding a message transmitted by the client module, with a second key associated with the destination module; decodes the stored first digital signal with the first key, taking into account at least part of the use restriction

information, into a second digital signal representing at least part of the first digital signal module (column 1, lines 60-67: " stores the current encryption/decryption algorithms and keys for parties registered with the network secure communications gateway.." Figure 2: column 3, lines 35-53: "node A is the client and node B is the destination.. file is transferred to A's network server interface, where a decision can be executed to send the file encrypted.." and Figure 2: column 3, lines 54-column 4, line 3: "if B is a client, B's algorithm and key are loaded into the encryption server and encrypted file... at node B the encrypted file is identified as a file having been sent from the encryption gateway, appropriate decryption algorithm and key are used to decrypt the file..." and Abstract: "node A encrypted the message using party A's secret key and encryption algorithm, copies of which are stored at the network gateway... Party A sends the encrypted message, addressed to party B, initially to the gateway. The gateway decrypts the message, using party A's secret key and algorithm and then encrypted the decrypted message using party's B secret key and algorithm.." and column 3, 1-34: "decryption server decrypts the encrypted message from node A using node A's algorithm and key and the plain text file is conveniently buffer stored in buffer..").

Regarding Claim 21, Ross teaches a method for the transfer of at least one digital signal according to Claim 20, wherein the destination module comprises a destination server connected to the network and at least one destination client connected to the destination server (Figure 1).

Regarding Claim 22, Ross teaches a method for the transfer of at least one digital signal according to Claim 21, wherein at least part of the second digital signal is transferred to at least one of the destination stations (Figure 1 and column 2, lines 30-column 3, line 23)..

Regarding Claim 23, Ross teaches a method for the transfer of at least one digital signal according to Claim 21, wherein the second key is associated with the destination server (Abstract: "node A encrypted the message using party A's secret key and encryption algorithm, copies of which are stored at the network gateway... Party A sends the encrypted message, addressed to party B, initially to the gateway. The gateway decrypts the message, using party A's secret key and algorithm and then encrypted the decrypted message using party's B secret key and algorithm..").

Regarding Claim 26, Ross teaches a method for the transfer of at least one digital signal according to Claim 20, wherein upon reception of a request to transfer the first digital signal encoded with the first key to at least one second destination module, the destination module: obtains a third key associated with the at least one second destination module; encodes the first key and information for the restriction on the use of the at least one second destination module, with the third key; transfers the first digital signal encoded with the first key to the destination module; transfers the first key

and use restriction information encoded with the third key to the at least one second destination module (column 1, lines 60 – column 2, line 10: "keys for parties registered with the network secure communication gateway.. multiple keys are being used.. the secure communications gateway periodically changes client keys to provide additional system security..").

Ross doesn't specifically state restriction forms part of the group of restrictions on the duration of authorization for the display of the at least one digital signal by the destination station, the storage of the at least one digital signal by the destination station and the printing of the at least one digital signal by the destination station and restriction forms part of the group of restrictions on the duration of authorization for the display of the at least one digital signal by the destination station, the storage of the at least one digital signal by the destination station and the printing of the at least one digital signal by the destination station.

Regarding Claim 7, Herpel discloses a method according to Claim 2, wherein the information representing at least one restriction forms part of the group of restrictions on the duration of authorization for the display of the at least one digital signal by the destination station, the storage of the at least one digital signal by the destination station and the printing of the at least one digital signal by the destination station ([0013]: "usage rights information and the content item itself allows to establish procedures, maintaining tight control over the ability to use it..").

Regarding Claim 9, Herpel discloses a method according to Claim 8, wherein the first digital signal representing media content data is at a first resolution and in that the destination server device also determines the whether information representing at least one restriction associated with at least one destination station has been transferred by the client server device and, if so, generates the second decoded digital signal at a resolution lower than the first resolution of the first digital signal representing media content data ([0013]: "watermarking for resolution" and [0017]: secure communication channel should be used between the devices... [0014]: "multimedia content item itself is copied to the secondary device, if it is not yet present there.. content descriptor is copied to the secondary device".. [0013]: "usage rights information").

Regarding Claim 10, Herpel discloses a method according to Claim 9, wherein the destination server device also determines whether information representing the at least one restriction has been transferred by the client server device and, in the negative, the destination server device transfers the second digital signal representing the whole of the first digital signal ([0013]: "watermarking for resolution" and [0017]: secure communication channel should be used between the devices... [0014]: "multimedia content item itself is copied to the secondary device, if it is not yet present there.. content descriptor is copied to the secondary device".. [0013]: "usage rights information").

Regarding Claim 15, Herpel teaches a method for the transfer of at least one digital signal according to Claim 13, wherein the restriction use information comprises information for the restriction on the use of the digital signal by the at least one destination client, for which the digital signal is intended ([0013]: "usage rights information and the content item itself allows to establish procedures, maintaining tight control over the ability to use it..").

Regarding Claim 16, Herpel teaches a method for the transfer of at least one digital signal according to Claim 12, wherein the use restriction information comprises the specification of rights for copying or storing or reproducing or printing the at least one digital signal, the time validity of said rights, the specification of the resolution under which the digital signal should be accessed ([0013]: "usage rights information and the content item itself allows to establish procedures, maintaining tight control over the ability to use it.. to copy the actual multimedia content item freely while maintaining control over the ability to use it.. and [0021]").

Regarding Claim 24, Herpel discloses a method for the transfer of at least one digital signal according to Claim 21, wherein the restriction use information comprises information for the restriction on the use of the first digital signal by the at least one destination client, for which the digital signal is intended intended ([0013]: "usage rights information and the content item itself allows to establish procedures, maintaining tight control over the ability to use it..").

Regarding Claim 25, Herpel discloses a method for the transfer of at least one digital signal according to Claim 20, wherein the use restriction information comprises the specification of rights for copying or storing or reproducing or printing the at least one digital signal, the time validity of said rights, the specification of the resolution under which the digital signal should be accessed ([0013]: "usage rights information and the content item itself allows to establish procedures, maintaining tight control over the ability to use it.. to copy the actual multimedia content item freely while maintaining control over the ability to use it.. and [0021]").

The examiner notes that one of ordinary skill in the art at the time the invention was made would have modified the teachings of Ross to information representing at least one restriction forms part of the group of restrictions on the duration of authorization for the display of the at least one digital signal by the destination station, the storage of the at least one digital signal by the destination station and the printing of the at least one digital signal by the destination station taught in Herpel. Manages the rights associated to a multimedia content item in order to satisfy both the legitimate rights of the content author or rights owner and the legitimate user of such content. In the time of mass storage devices that can be used as media servers, this requires easy ways to move content as well as the rights to use it, the usage license. Moving the rights to a new location implies that the item at its new location is now the legitimate

original version that may be played back or form which one further copy may be derived. (Herpel: Abstract)

Claims 27-60

The device, method claims and computer program product are one of the same therefore rejected for the same reason as the method claims above.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Alboulhosn et al. (US 6, 938, 042 B2) teaches peer-to-peer file sharing.

Pabla et al. (US 7, 127, 613 B2) teaches secured peer-to-peer network data exchange.

Kawamoto (US 7, 076, 654 B2) teaches multicast system, authentication server terminal, multicast receiver terminal controlling method and storage medium.

Kobata et a. (US 2002/0077985 A1) teaches controlling and managing digital assets.

Bryan et al. (US 2003/0084280 A1) teaches secure file transfer and secure file transfer protocol.

Messerges et al. (US 2004/0103312 A1) teaches domain-based digital-rights management system with easy and secure device enrollment.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kari L. Schmidt whose telephone number is 571-270-1385. The examiner can normally be reached on Monday - Friday: 7:30am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KS

TAGHI ARANI
PRIMARY EXAMINER
6/22/07